

ルーティングセキュリティへの道

Matsuzaki 'maz' Yoshinobu

<maz@iij.ad.jp>



2009/11/25

Copyright (c) 2009 Internet Initiative Japan Inc.



2009/11/25

Copyright (c) 2009 Internet Initiative Japan Inc.



2009/11/25

Copyright (c) 2009 Internet Initiative Japan Inc.







2009/11/25

Copyright (c) 2009 Internet Initiative Japan Inc.

/

守りたいモノ

- ユーザがよろしく通信できる環境
 - 環境を作ってるのが経路制御
- 経路制御を守らなきゃいけない
 - そうすると、結果的にユーザがよろしく通信できる
 - 変なところにも行かなくて済む

何から守るか

- 心配しだすとキリがない
 - 費用対効果
- 段々心配事は増えていく
 - 時代に応じたちょうど良さが求められる
- 現実的に起こりそうなリスクを押さえていく
 - 現時点＋近い将来 程度
 - 意図した経路制御を維持できるように

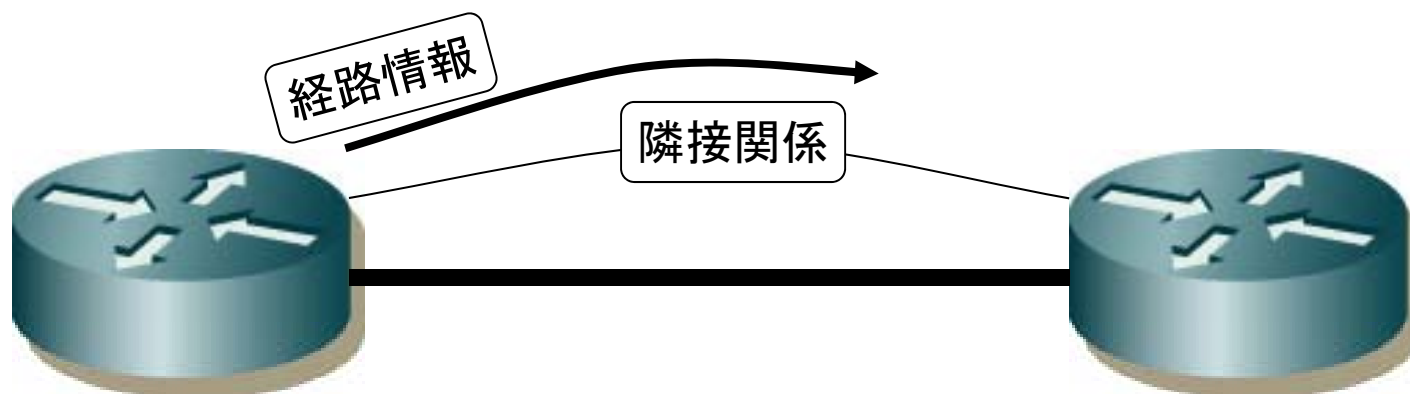
経路制御への脅威

- ほとんどミスオペ、ときどき攻撃
 - 素早く検知
 - 影響を閉じ込める
 - 速やかな復旧
 - ミスを軽減する環境づくり
- BGPではミスが伝搬しやすい

経路制御を考えてみる

- 経路制御には一意なリソースが必要
 - まずはリソースの確保
 - IPアドレス(prefix)
 - AS番号
- インターネットでは、IR(Internet Registry)によってリソースの一意性を担保している
 - APNIC, JPNICなど
 - 登記所としての機能

一般的な経路制御



- 何らか隣接関係を利用して、経路情報を交換

経路制御全般の脅威

- 隣接関係
 - 間違った隣接関係が構築される
 - 勝手に切断される
 - なりすましに騙される
- 経路情報
 - 間違った経路情報が流れる
 - 意図しない経路制御になる
 - 機器の処理能力を超える

BGPの隣接関係

- TCPセッションを頑張って守る
 - md5認証
 - IPSEC
 - GTSM(Generalized TTL Security Mechanism)
 - IP TTL 255のパケットで隣接だと判断
- 今のところ、md5認証が多用されている
 - 完全性や機密性より、とりあえずの認証
- 他組織と接続するときに事前の交渉ができる

BGPは経路情報のほうが問題

- 今時はほとんどの経路情報をBGPで処理
 - 経路制御の多くを担う
- しかも他の組織と経路情報を交換する
 - 直接の接続先は知っている
 - でもその先は知らない組織
 - 信頼できない組織からの経路情報も受け取る

BGPの経路情報

- prefix+パス属性
- 経路制御に関わる主なパス属性
 - origin
 - as_path
 - nexthop
 - med
 - local preference
 - bgp community

BGPで死守すべき経路情報

- ピアを張っているIPアドレス
 - 大抵の場合、IGPでも広報
 - 同じprefix長であればIGPが優先される場合が多い
- BGP経路のnexthopになっているIPアドレス
 - 絶対に外部から受け取ってはいけない
 - 全eBGPで確実にprefixフィルタを実装
 - more specific経路にも注意
 - bgp nexthopになりうるIPアドレス
 - 経路を生成しているルータ
 - 相互接続アドレス
 - IXやプライベートピア

他のASから広報されるパス属性

- 受信側でポリシーがあるなら、きちんと対応
 - 最低限、どうしているか確認してみましょう
- パス属性によって、伝搬範囲が異なる
 - local preferenceなど、絶対に他のASから広報されないパス属性もある
- 思わぬパス属性が広報されても、意図しない経路制御にならないように

med

- 隣接のASが値を設定する
 - 担当者と交渉できる
- AS内のポリシー
 - deterministic med
 - always compare med
- ASのポリシーに応じて対応
 - そのまま受信して評価
 - 問答無用で値の上書き or 値の付け足し

bgp community

- もしかしたら遠方のASが付与した値が伝搬してくるかも
 - 何が付いてくるかわからない
- トランジット経路の識別など、内部の経路制御に利用している場合は、対応が必要
 - 該当communityの削除
 - 問答無用で上書き

経路フィルタ

- 不正経路を伝搬させない
 - ミスオペや攻撃の影響範囲を小さく
- Prefixやパス属性に基づいて選択
 - 属性フィルタは独立している場合が多い
 - as_pathならas_pathのみのフィルタ
 - prefix+パス属性に適切に対応できていない
 - フィルタ運用上の課題
- それでも、とても有効な手段


対カスタマへの経路フィルタ

- 経路がインターネットに伝搬するポイント
 - ここで不正広報を止められれば、影響も少ない
- どんな経路が広報されるか、事前に分かる
 - prefixや広報元のASなど
- トランジットする経路は厳密にフィルタ
 - お客様からの経路受信時にフィルタを適用

対ピア、アップストリーム

- どんな経路が広報されるか分からない場合も
 - 巨大なASになると、接続などの変更が多発
- できる限りの経路フィルタ
 - 自身の経路制御ポリシーを乱されないように

ピアとの受信フィルタ運用(2008年)

- prefixベースの経路フィルタ
 - 必要ない経路を受け取らない最小限のフィルタ
 - Martian, default, IJ PAなどを受け取らない
- as_pathベースの経路フィルタ  問題児
 - 事前に連絡のあったAS Pathのみ受信する
 - 基本的にメールで連絡しあう
- 受信prefix数制限

当時のas_pathフィルタ運用の問題点

- メールでの連絡
 - ツールとの親和性の悪さ
 - 人的ミスの懸念
- copy & pasteが前提になっていた
 - みんな $^(2497_)+\$$ みたいな形式で連絡
 - 4 octet ASどうする？
- やっぱり何か自動化の仕組みを作りたい
 - IRR (Internet Routing Registry)があった！

IIJとIRR

- 昔々
 - Policy Routing DataBase (PRDB)にnetnumを登録
 - 登録しないと届かないネットワークがあった
- 1995年～
 - RADBに移行
- 2003年～
 - MAINT-AS2497の認証を全てPGPに移行
- 2005年～
 - JPIRRにも同様の内容で登録開始

IRRを利用した試行

- みんなが運用できる事を考える
 - as-set程度であれば、更新を維持できるはず
- それを利用すれば自動化できる
 - 与えられたas-setから再帰的にIRRを検索し、広報される経路のorigin ASのリストを作成
 - private ASを除外する等の追加
- 幾つかのISPとやってみた
 - ちゃんと動く



2008年7月7日

今日は約束の7月7日です。AS Path Update連絡終了のお知らせです。

これまでIJJはピアに対して広報する経路の変更点をAS Path形式にてメールで連絡していました。またピアからご連絡頂いたAS Pathからフィルタを生成し、IJJ側での経路受信フィルタとして適用していました。しかしながら手作業によるミスや更新洩れの懸念、4 octets ASの登場などを考慮すると今後は別な手法で経路フィルタを実施すべきだろうとの結論に至りました。

既に個別にはご連絡しておりますが、本日、2008年07月07日をもって基本的にAS Pathの更新連絡を終了致します。

本日以降は基本的に以下の様なフィルタを受信経路に適用します。

1. 指定頂いたas-set objectから生成するorigin ASでのAS Pathフィルタ
2. プライベート空間等、不正だと思われる経路へのprefixフィルタ
3. 受信prefix数の最大値制限

変更後の受信フィルタ

- as-setからorigin ASベースのフィルタを生成
 - 各ASからフィルタ生成用のas-setをご連絡頂く
 - そこから _2497\$ の様なフィルタを生成
- 週一程度を目途に更新
 - 緊急時には別途ご連絡頂ければ個別に対応

良かった事や問題点

良かった

- 運用が楽に
 - 連絡の状態管理が不要
 - 運用コストの削減
- チェックシステムの充実
 - IRRを見てれば良い

課題

- IRR自体の問題
 - 名前空間
 - 信頼性
- 運用上の問題
 - 他のASの設定状況
 - コンタクトアドレスの定期的な到達性チェック

AS内は守れそう

- 既存の手法を組み合わせることで、内部の経路制御はある程度、意図通りになりそう
 - 適切な経路フィルタを適用
 - パス属性のチェック
- 経路制御の正しさをチェックできる
 - 何せ自分が一番良くわかっている(はず)

問題はASの外

- 何せユーザは“インターネット”を期待する
 - 僕だって期待する
- 手の届かないところで制御されている経路
 - 他のASが受信している経路
 - 他のASから広報されてくる経路

他のASが受信している経路

- 自身のprefixが別なASから広報された場合
 - それを最適経路だと思ったASとは通信できない
 - more specific
 - as_path長で近傍に見える
 - 検出には他のASの協力が必要
 - 今のところ、未然に防ぐ手段はない
- メールや電話で連絡して、広報停止を依頼
 - IRのwhois情報などでこちらの正当性を主張する

他のASから広報される経路

- 正当性の確認が難しい
 - 正当性の根拠として使える情報が無い
 - RADBなどは、不正確な登録情報が多い
 - JPIRRのみが抜群に頑張ってる
 - 次点はRIPE DBかなあ
- どこまで確認したいかも問題
 - 実装するなら、ある程度の期間は安心してほしい

まとめ

- まずは自分のできる範囲を
 - 自身の経路制御ポリシーを守る
 - 自身の広報/トランジットする経路はばっちり確認
 - IRやIRRなどの登記情報もきちんと更新
- 世界を巻き込んで、インターネットの経路制御を良くしていくことが課題